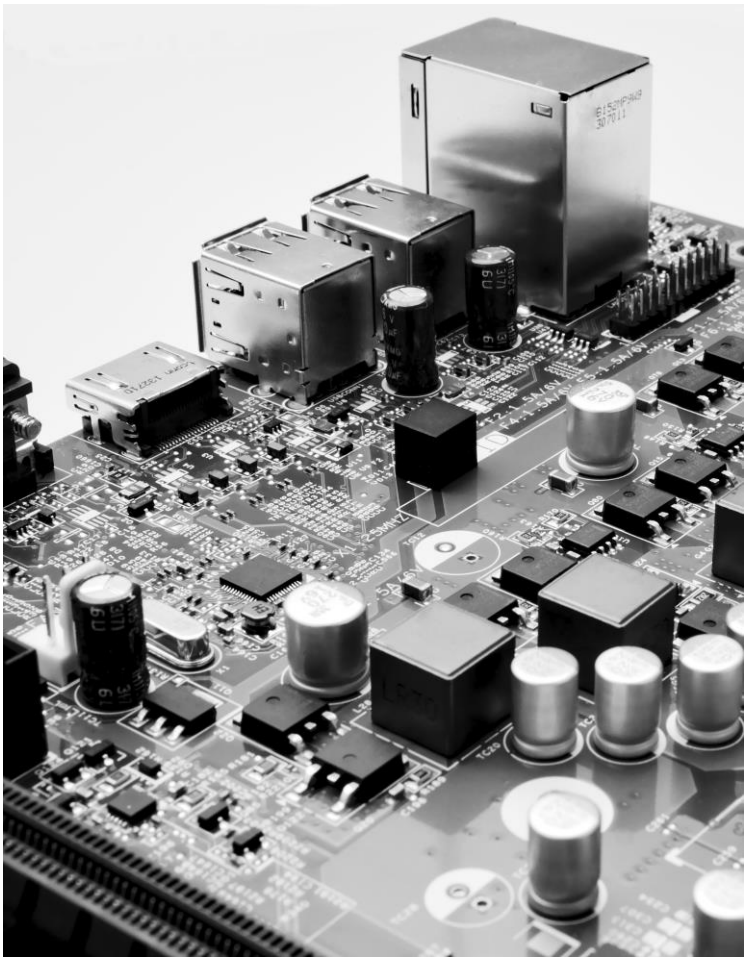

ASSIGNMENT 1

ITRI 615

ABSTRACT

This is an executive summary of 2 related scientific articles regarding the integrity aspect in cloud computing.

Enrico Dreyer

31210783

Table of Contents

Background

When looking at information security, integrity is the correctness and absoluteness of data. An integrity policy declares access restrictions, that protect data from inappropriate modification, but only when correctly and successfully imposed.

Introduction

Since data is getting bigger and the need to access that data from many devices, small to medium organizations are moving their data to cloud services. This data needs to be confidential and preserve integrity. These organizations want to focus less on their IT infrastructure, and more on their business process so that they can increase profit. This is why cloud computing is increasing in popularity and such an important role in the modern market.

Cloud security issues

Cloud computing security is a wide topic and includes the control to protect data, infrastructure, and services. By outsourcing data, the user loses physical control over data. This increases many threats facing cloud computing not just from an outsider but also from an insider that can utilize cloud amenability to harm. This can risk data integrity.

Integrity Requirements and Limitations

Even if the attacker can not steal the information, they can still remove, add, or change fragments of the data. Data in the cloud should be reliable, accurate, and uncorrupted.

Attacks in the cloud computing environment

Cloud computing gets exposed to many attacks. Several types of attacks that threaten data integrity:

- Cloud Malware Injection attack
- Authentication attack
- User to root attack
- Attack on virtualization
- Side-Channel Attack

Threats to cloud computing

Data loss

When companies outsource all their data, they expose their important data and risk it from being lost due to malicious attacks, server crashes, or accidental deletion by their cloud service provider.

Data breaches

When customers use the same virtual machine, due to multi-tenancy, they could share the same database and corrupt each other's data.

Malicious insiders

Malicious insiders are database administrators, or employees of the company offering their cloud services, that are authorized to manage data. They can corrupt or steal the data to hurt a certain company.

Insecure interface and APIs

Communication between the client and the cloud service provider is done through API calls. The interface should prevent unauthorized access. This can be done by understanding the dependencies of the API.

Data integrity Issues

Since the computation and data that is outsourced to remote servers, maintenance of data integrity should be checked continuously. This means that data should be safe from any unauthorized modifications and any deviation from normal activity should be detected.

Data manipulation or loss

Users have large amounts of files, this is why provides have Storage as Service (SaaS). These files can be changed accidentally or intentionally. This can happen when restoring the incorrect backup or when an attacker utilized the user's source data since they lost control over it.

Protecting data integrity

Encryption provides good confidentiality against attacks from a cloud provider but does not protect data from corrupted from software bugs or configuration errors.

Traditional ways of proving the integrity of data

First is using the message authentication code algorithm, by downloading the file and checking the hash value. The second is by use of a hash tree, then calculating the hash value in the cloud. When the owner of the data wants to check the integrity of his data, he can just ask for the root value and compare it to the one that he has.

Provable Data Possession (PDP)

This scheme is used to statically investigate the correctness of data that is outsourced to cloud storage without the need to receive the data. The model is designed to check that the data that is stored, is still in its possession and that the server still has the original data.

PDP detects when a large amount of data gets corrupted and can be verified privately or publicly.

Proof of Retrievability

This is a cryptographic approach that is based on a challenge-response protocol where a chunk of the data is shown to be unbroken and retrieved without it being retrieved from the cloud. The simplest form is taking a hash block and using a keyed hash function.

Conclusion

The cost of cloud computing is cheaper than building your own IT infrastructure. However, this price comes with many security issues and has more to come as the technology matures. This security issue is related not just to integrity, but also confidentiality and the availability of data when it is needed. In this executive summary, I mentioned some techniques to protect data integrity that will lead to cloud storage being more secure.

References

Abdul-Jabbar, S.S., Aldujaili, A., Mohammed, S.G. and Saeed, H.S., 2020. Integrity and Security in Cloud Computing Environment: A Review. Journal of Southwest Jiaotong University, 55(1).

Aldossary, S. and Allen, W., 2016. Data security, privacy, availability and integrity in cloud computing: issues and current solutions. *International Journal of Advanced Computer Science and Applications*, *7*(4), pp.485-498.